Cisco ASA – FirePower

ASA Firewall – Course Content

FIREWALLS – OVERVIEW

- Firewall Vendors
- ASA firewalls – Models

CISCO ASA FIREWALL

- MANAGING CISCO ASA FIREWALL
- LAB: Basic ASA Configuration
- LAB: ASA BASIC INTERFACE CONFIGURATIONS.

ASA – ROUTING

- ASA –Static & Default Routing
- LAB: ASA Routing using RIPv2
- LAB: ASA Routing using EIGRP
- LAB: ASA Routing – OSPF
- LAB: Redistribution

ASA – ACCESS CONTROL LIST

- LAB: ASA Security policies & ACL
- ACL OBJECTGROUP
- LAB: ACL & object groups
- LAB; Time Based ACL

Remote Access on ASA

- Using Telnet
- Using SSH
- How to Run ASDM over ASA using GNS3

NETWORK ADDRESS TRANSLATION

- LAB: NAT (Dynamic NAT)
- LAB: NAT (Dynamic PAT)
- LAB: NAT (Dynamic PAT using Exit Interface)
- LAB: Dynamic NAT/PAT combination:
- LAB: Static NAT:
- LAB: STATIC PAT:

Cisco ASA – FirePower

ASA Layer 2 options

- LAB: ADDDING Sub-interfaces on ASA.
- Lab: Ether-channel on ASA

ASA Security Contexts (virtual Firewalls)

- Creating security contexts / Virtual Firewalls

ASA Failover

- Active / Standby Fail over
- Active / Active Fail over

ASA Clustering

- ASA clusters – spanned Mode

Transparent Layer 2 Firewall

- Basic L2 firewall configuration
- Routing via L2 firewall
- Ethertype ACL

ASA deep packet Inspection

- ASA deep packet Inspection – Overview
- ICMP Inspection
- FTP on non-standard port

Site to Site VPN – ASA

- ASA VPN - Lab Setup
- ASA Site to Site VPN
- LAB - SITE-TO-SITE IPSEC VPN (ASA)
- LAB - SITE-TO-SITE IPSEC VPN (ASA) – ASDM Setup Wizard
- LAB - SITE-TO-SITE IPSEC VPN (ASA) – ASDM Configuration
- LAB:IPSEC WITH NAT EXEMPTION (ASA)
- ASA – Site to site VPN – Dynamic IP
- LAB: Site-to-Site IPSEC VPN with Dynamic IP (ASA)
- IPSEC VPN between Cisco ASA and Cisco Router
- IPSEC VPN between Cisco ASA and Cisco Router (Dynamic IP)

ASA Remote Access VPN – SSL VPN

- What is SSL VPN ?
- LAB - SSL VPN – ASA - CLI Configuration
- LAB: SSL Clientless VPN – Verify via ASDM
- LAB : Clientless SSL VPN – ASDM Setup Wizard

Cisco ASA – FirePower

- SSL Clientless VPN – Configuration with ASDM
- Clientless SSL VPN – Bookmarks
- LAB - Clientless SSL VPN – Alias
- LAB - Clientless SSL VPN – Tunnel Group URL
- Clientless SSL VPN – Monitoring
- Clientless SSL VPN – Disable Auto-capablities
- Clientless SSL VPN – Bookmarks with FQDN
- SSL VPN – Thin Client – Port Forwarding
- Clientless SSL VPN – Port Forwarding
- SSL VPN – Thin Client - Smart Tunnels
- LAB – SSL VPN Thin Client – Smart tunneling
- Client Based SSL VPN – Anyconnect VPN
- LAB - SSL Anyconnect VPN
- Connect to Cisco anyconnect VPN client windows 10

The Securing Networks with Cisco Firepower v1.0 (SNCF 300-710) exam is a 90-minute exam associated with the CCNP Security, and Cisco Certified Specialist – Network Security Firepower certifications.

This course will help you:

- Implement Cisco Firepower Next-Generation IPS to stop threats
- Address attacks
- Increase vulnerability prevention against suspicious files
- analyze for not-yet-identified threats
- Gain leading-edge skills for high-demand responsibilities focused on security
- How to use and configure Cisco Firepower Threat Defense technology
- Beginning with initial device setup
- Configuration - Routing, High availability
- Cisco ASA to Firepower Threat Defense migration
- Traffic control
- Network Address Translation (NAT)

The course will then explore how to implement advanced Next-Generation Firewall (NGFW) and Next-Generation Intrusion Prevention System (NGIPS) features,

- including network intelligence,
- file type detection,
- network-based malware detection,
- deep packet inspection.

Students will also learn how to

Cisco ASA – FirePower

- Configure site-to-site VPN,
- Remote-access VPN,
- SSL decryption before moving on to detailed analysis, system administration, and troubleshooting.

This course combines lecture materials and hands-on labs throughout to make sure that students are able to successfully deploy and manage the Cisco Firepower system.

After you pass 300-710 SNCF:

- You earn the Cisco Certified Specialist - Network Security Firepower certification.
- You will have satisfied the concentration exam requirement for new CCNP Security certification.
- To complete CCNP Security, you also need to pass the Implementing and Operating Cisco Security Core Technologies (350-701 SCOR) exam or its equivalent.

Course prerequisites

- Knowledge of TCP/IP and basic routing protocols, and familiarity with firewall, VPN, and IPS concepts

Course objectives

Upon completion of this course, you should be able to:

- Describe key concepts of NGIPS and NGFW technology and the Cisco Firepower Threat Defense system,
- Identify deployment scenarios
- Perform initial Firepower Threat Defense device configuration and setup tasks
- Describe how to manage traffic and implement Quality of Service (QoS) using Cisco Firepower Threat
- Defense
- Describe how to implement NAT by using Cisco Firepower Threat Defense
- Perform an initial network discovery, using Cisco Firepower to identify hosts, applications, and services
- Describe the behavior, usage, and implementation procedure for access control policies
- Describe the concepts and procedures for implementing security Intelligence features
- Describe Cisco AMP for Networks and the procedures for implementing file control and Advanced Malware
- Protection
- Implement and manage intrusion policies
- Describe the components and configuration of site-to-site VPN
- Describe and configure a remote-access SSL VPN that uses Cisco AnyConnect®
- Describe SSL decryption capabilities and usage

Course outline

- Cisco Firepower Threat Defense Overview
- Firepower NGFW Device Configuration

Cisco ASA – FirePower

- Firepower NGFW Traffic Control
- Firepower NGFW Address Translation
- Firepower Discovery
- Implementing Access Control Policies
- Security Intelligence
- File Control and Advanced Malware Protection
- Next-Generation Intrusion Prevention Systems
- Site-to-Site VPN
- Remote-Access VPN
- SSL Decryption
- Detailed Analysis Techniques
- System Administration
- Firepower Troubleshooting

Lab Outline

- Lab 1: Initial Device Setup
- Lab 2: Device Management
- Lab 3: Configuring High Availability
- Lab 4: Migrating from Cisco ASA to Firepower Threat Defense
- Lab 5: Implementing QoS
- Lab 6: Implementing NAT
- Lab 7: Configuring Network Discovery
- Lab 8: Implementing an Access Control Policy
- Lab 9: Implementing Security Intelligence
- Lab 10: Implementing Site-to-Site VPN
- Lab 11: Implementing Remote Access VPN
- Lab 12: Threat Analysis
- Lab 13: System Administration
- Lab 14: Firepower Troubleshooting